REMARKS

The present application was filed on October 16, 2000 with claims 1-23. Claims 1-23 are currently pending in the application. Claims 1, 7, 18 and 22 are the independent claims.

In the Office Action, claims 7-10, 22 and 23 are rejected under 35 U.S.C. §102(b) as being anticipated by Kumar et al., "Coding for Blacklisting Problems Without Computational Assumptions" (hereinafter "Kumar"). In addition, claims 1-4, 6, 7, 11-13, 18, 19, 21 and 22 are rejected under U.S.C. §103(a) as being unpatentable over Gafni et al., "Efficient Methods for Integrating Traceability and Broadcast Encryption" (hereinafter "Gafni") in view of Wallner et al., "Key Management for Multicast: Issues and Architecture" (hereinafter "Wallner"). Finally, claims 5, 14-17 and 20 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gafni in view of Wallner and further in view of Kumar.

In this response, Applicants traverse the §102(b) and §103(a) rejections. Applicants respectfully request reconsideration of the present application in view of the following remarks.

With respect to the §102(b) objection, Applicants initially note that the Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(a) specifies that a reference is qualified as prior art under 35 U.S.C. §102(b) "[i]f the publication or issue date of the reference is more than 1 year prior to the effective filing date of the application." Applicants also note that this MPEP section further provides that "[t]he examiner must determine the issue or publication date of the reference so that a proper comparison between the application and reference dates can be made." Finally, the MPEP §2128.02 states:

> A publication disseminated by mail is not prior art until it is received by at least one member of the public. Thus, a magazine or technical journal is effective as of its date of publication (date when first person receives it) not the date it was mailed or sent to the publisher. In re Schlittler, 234 F.2d 882, 110 USPQ 304 (CCPA 1956).

In reference to the above criteria for the qualification of a §102(b) reference, Applicants respectfully submit that the Examiner has failed to show that Kumar was published and received by one member of the public more than one year prior to the effective filing date of the present

application. Therefore, the Examiner has failed to establish that Kumar is a §102(b) reference with respect to claims 7-10, 22 and 23.

Applicants wish to further submit that Kumar does not anticipate claims 7-10, 22 and 23. The MPEP, §2131, specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). For the reasons identified below, Applicants submit that the Examiner has failed to establish anticipation of at least independent claims 7 and 22 by the Kumar reference.

Each of independent claims 7 and 22 includes a step comprising "updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold." The Examiner, in formulating the §102(b) rejection, argues that the Kumar reference on page 616, "3 The Overall Construction," paragraph 2, anticipates these claims when it discusses a broadcast encryption scheme:

> The pieces [of the encrypted broadcast] corresponding to keys belonging to users who have been excluded are then discarded, and the remaining encrypted pieces are broadcast to all users. By decrypting the pieces corresponding to the keys that each valid user has, the user reconstructs the original message M.

Applicants respectfully submit that this language in Kumar fails to teach or suggest the updating of subscriber keys as recited in claims 7 and 22. As a result, the Kumar reference fails to show an element of the claimed invention and fails to provide its associated benefits in terms of an enhanced long-lived broadcast encryption method.

The Examiner, in making his §102(b) rejection, further asks Applicants to "[a]lso see page 617 'The Outer Code'" in Kumar. (Office Action, page 3). However the Examiner provides no

explanation why the cited portion of the reference is relevant. Applicants respectfully submit that this portion of the reference has no application to the claimed invention.

Therefore, since each of independent claims 7 and 22 includes at least one element not described in Kumar, these claims are not anticipated by Kumar. Dependent claims 8-10 and 23 are believed allowable for at least the reasons identified above with regard to their respective independent claims.

With regard to the §103(a) rejections, Applicants note that a proper *prima facie* case of obviousness requires that the cited references, when combined, must "teach or suggest all the claim limitations," and that "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." See MPEP § 706.02(j). Applicants further note that MPEP §2145 states that "[i]t is improper to combine references where the references teach away from their combination," citing In re Grasselli, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983). "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." In re Gurley, 27 F.3d 551, 553, 31 USPQ2d 1130 (Fed. Cir. 1994).

Independent claims 1, 7, 18 and 22 each include steps comprising modifying or adjusting the set of broadcast keys by excluding compromised subscriber keys and "updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold." The Examiner, in formulating the §103(a) rejection, acknowledges that Gafni "does not explicity teach 'modifying...' or 'updating...,'" but argues that these missing teachings are provided by Wallner. (Office Action, pages 4-5). The Examiner further argues that it would be obvious to one having ordinary skill in the art to use Wallner's method in combination with Gafni's method because "[o]ne would have been motivated to do so since Gafni suggested making this modification." (Office Action, page 5). The Applicants respectfully disagree. As discussed below, Gafni contains language that, in fact, teaches away from such combination.

The Examiner looks to page 377, 3rd complete paragraph of Gafni for the motivation to combine Gafni and Wallner. This paragraph states:

> A quite different approach to solving the problem of broadcast encryption appears in [Wallner]. The model differs from all of the above mentioned works in that when some user is removed from the system, keys of existing users are updated (called *rekeying*). In [Wallner], a hierarchical tree-based scheme is recommended for use in a broadcast encryption system. The system is maximally resilient but not fully scalable.

By describing Wallner as "[a] quite different approach," Gafni suggests that Wallner is a divergent approach from his own, thereby teaching away from a Gafni-Wallner combination. In addition, Gafni suggests Wallner's method is inferior to his own by describing Wallner's methods as "maximally resilient but not fully scalable." In comparison, Gafni describes his own method as "both maximally resilient and fully scalable." (Gafni, p. 378, 1st paragraph). Gafni thereby discourages the use of Wallner's method. Finally, later in the reference, Gafni notes that he will "not consider other models such as . . . schemes that allow rekeying," referring to Wallner. (Gafni, p. 378, 1st paragraph). Taken as a whole, such teaching away is believed to constitute strong evidence of non-obviousness.

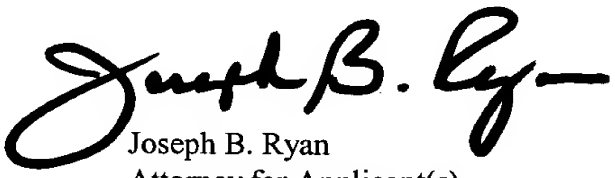
Applicants therefore respectfully submit that independent claims 1, 7, 18 and 22 are allowable over Gafni in view of Wallner.

Dependent claims 2-4, 6, 11-13, 19 and 21 are believed allowable for at least the reasons identified above with regard to independent claims 1, 7 and 18. These dependent claims are also believed to specify additional separately-patentable subject matter.

With regard to the additional §103(a) rejection of dependent claims 5, 14-17 and 20 with reference to the Gafni-Wallner combination further in view of Kumar, the Kumar reference fails to supplement the above-described fundamental deficiencies of Gafni and Wallner as applied to claims 4, 12 and 19. It is further noted that Examiner asserts that Kumar contributes to the Gafni-Wallner combination because Kumar teaches tracking and updating subscriber keys when a predefined threshold is met. Applicants wish to reassert their disagreement with this conclusion as stated above in the Applicants' remarks concerning Kumar as a §102(b) reference.

In view of the above, Applicants believe that claims 1-23 are in condition for allowance, and respectfully request the withdrawal of the §102(b) and §103(a) rejections.

Respectfully submitted,



Date: April 30, 2004

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517